IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re application of :

Ryogo YANAGISAWA :

Serial No. NEW : **Attn: APPLICATION BRANCH**

Filed March 26, 2004 : Attorney Docket No. 2004_0472A

PUBLIC KEY GENERATION APPARATUS, SHARED KEY GENERATION APPARATUS, KEY EXCHANGE APPARATUS, AND KEY EXCHANGING METHOD :

THE COMMISSIONER IS AUTHORIZED TO CHARGE ANY DEFICIENCY IN THE FEES FOR THIS PAPER TO DEPOSIT ACCOUNT NO. 23-0975

CLAIM OF PRIORITY UNDER 35 USC 119

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Sir:

Applicant in the above-entitled application hereby claims the date of priority under the International Convention of Japanese Patent Application No. 2003-088788, filed March 27, 2003, as acknowledged in the Declaration of this application.

A certified copy of said Japanese Patent Application is submitted herewith.

Respectfully submitted,

Ryogo YANAGISAWA

By _____
Jeffrey R. Filipek
Registration No. 41,471
Attorney for Applicant

JRF/fs
Washington, D.C. 20006-1021
Telephone (202) 721-8200
Facsimile (202) 721-8250
March 26, 2004

日本国特許庁
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出願年月日
Date of Application: ２００３年　３月２７日

出願番号
Application Number: 特願２００３－０８８７８８

[ST. 10/C]: [ＪＰ２００３－０８８７８８]

出願人
Applicant(s): 松下電器産業株式会社

２００３年　７月２２日

特許庁長官
Commissioner,
Japan Patent Office 今井康夫

出証番号　出証特２００３－３０５８０１７

【書類名】　特許願
【整理番号】　2037840200
【提出日】　平成15年 3月27日
【あて先】　特許庁長官殿
【国際特許分類】　H04L 9/08
【発明者】
　【住所又は居所】　大阪府門真市大字門真１００６番地　松下電器産業株式会社内
　【氏名】　柳澤　玲互
【特許出願人】
　【識別番号】　000005821
　【氏名又は名称】　松下電器産業株式会社
【代理人】
　【識別番号】　100081813
　【弁理士】
　【氏名又は名称】　早瀬　憲一
　【電話番号】　06(6395)3251
【手数料の表示】
　【予納台帳番号】　013527
　【納付金額】　21,000円
【提出物件の目録】
　【物件名】　明細書　1
　【物件名】　図面　1
　【物件名】　要約書　1
　【包括委任状番号】　9600402
【プルーフの要否】　要

【書類名】　明細書

【発明の名称】　公開鍵生成装置、共有鍵生成装置、鍵交換装置、及び鍵交換方法

【特許請求の範囲】

【請求項１】　乗算が定義された有限群Ｆ上の元をｇ、前記ｇの素数である位数をｑとし、０＜ｋａ＜ｑとなる乱数ｋａを生成する乱数生成手段と、

前記乱数ｋａと、前記元ｇと、前記素数ｑより、公開鍵ｙａを前記有限群Ｆ上で演算し出力する公開鍵生成手段とを備え、

少なくとも前記乱数生成手段と前記公開鍵生成手段とが同一の半導体集積回路上に集積され、

公開鍵配布元となる第１のユーザーの制御手段が、前記乱数生成手段と前記公開鍵生成手段とを制御して前記公開鍵ｙａを取得し、該公開鍵ｙａを公開鍵配布先となる第２のユーザーへ伝送する、

ことを特徴とする公開鍵生成装置。

【請求項２】　請求項１記載の公開鍵生成装置において、

前記公開鍵生成手段は、

前記乱数ｋａと、前記元ｇと、前記素数ｑより、前記公開鍵ｙａを、

ｙａ＝ｇ＾ｋａ　ｍｏｄ　ｑ

として、前記有限群Ｆ上で演算し出力する、

ことを特徴とする公開鍵生成装置。

【請求項３】　請求項１記載の公開鍵生成装置において、

前記有限群Ｆを有限体上の楕円曲線Ｅ（Ｆ）とし、前記楕円曲線Ｅ（Ｆ）の元をＧとし、

前記公開鍵生成手段が、前記乱数ｋａと、前記元Ｇと、前記素数ｑより、前記公開鍵ｙａを、

ｙａ＝ｋａＧ　ｍｏｄ　ｑ

として、前記楕円曲線Ｅ（Ｆ）上で演算し出力する、

ことを特徴とする公開鍵生成装置。

【請求項４】　請求項１ないし３のいずれかに記載の公開鍵生成装置におい

て、

前記乱数生成手段が、前記公開鍵ｙａの演算終了後に、新たな乱数を生成する、

ことを特徴とする公開鍵生成装置。

【請求項５】　乗算が定義された有限群Ｆ上の元をｇ、前記ｇの素数である位数をｑとし、０＜ｋａ＜ｑとなる乱数ｋａを生成する乱数生成手段と、

共有鍵配布先となる第２のユーザーが発生した０＜ｋｂ＜ｑとなる乱数ｋｂより生成された公開鍵ｙｂと、前記乱数ｋａより、共有鍵Ｋａを前記有限群Ｆ上で演算し出力する共有鍵生成手段とを備え、

少なくとも前記乱数生成手段と前記共有鍵生成手段とが同一の半導体集積回路上に集積され、

共有鍵配布元となる第１のユーザーの制御手段が、前記共有鍵配布先となる第２のユーザーより前記公開鍵ｙｂを取得し、前記乱数生成手段と前記共有鍵生成手段とを制御して、前記共有鍵Ｋａを導出する、

ことを特徴とする共有鍵生成装置。

【請求項６】　請求項５記載の共有鍵生成装置において、

前記共有鍵生成手段は、

前記共有鍵配布先となる第２のユーザーが生成した前記公開鍵ｙｂ＝ｇ＾ｋｂ　ｍｏｄ　ｑと、前記乱数ｋａにより、前記共有鍵Ｋａを、

Ｋａ＝ｙｂ＾ｋａ　ｍｏｄ　ｑ

として、前記有限群Ｆ上で演算し出力する、

ことを特徴とする共有鍵生成装置。

【請求項７】　請求項５記載の共有鍵生成装置において、

前記有限群Ｆを有限体上の楕円曲線Ｅ（Ｆ）とし、前記楕円曲線Ｅ（Ｆ）の元をＧとし、

前記共有鍵生成手段は、前記共有鍵配布先となる第２のユーザーが前記乱数ｋｂより前記楕円曲線Ｅ（Ｆ）上で演算し生成した前記公開鍵ｙｂ＝ｋｂＧ　ｍｏｄ　ｑと、前記乱数ｋａにより、前記共有鍵Ｋａを、

Ｋａ＝ｋａｙｂ　ｍｏｄ　ｑ

として、前記楕円曲線Ｅ（Ｆ）上で演算し出力する、

ことを特徴とする共有鍵生成装置。

【請求項８】　請求項５ないし７のいずれかに記載の共有鍵生成装置において、

前記乱数生成手段は、前記共有鍵Ｋａの演算終了後に、新たな乱数を生成する、

ことを特徴とする共有鍵生成装置。

【請求項９】　乗算が定義された有限群Ｆ上の元をｇ、前記ｇの素数である位数をｑとし、０＜ｋａ＜ｑとなる乱数ｋａを生成する乱数生成手段と、

前記乱数ｋａと、前記元ｇと、前記素数ｑより、公開鍵ｙａを前記有限群Ｆ上で演算し出力する公開鍵生成手段と、

共有鍵配布先となる第２のユーザーが発生した０＜ｋｂ＜ｑとなる乱数ｋｂより生成された公開鍵ｙｂと、前記乱数ｋａより、共有鍵Ｋａを前記有限群Ｆ上で演算し出力する共有鍵生成手段とを備え、

少なくとも前記乱数生成手段と前記公開鍵生成手段と前記共有鍵生成手段とが同一の半導体集積回路上に集積され、

共有鍵配布元となる第１のユーザーの制御手段が、前記乱数生成手段と前記公開鍵生成手段とを制御して前記公開鍵ｙｂを取得し、前記共有鍵生成手段を制御して前記共有鍵Ｋａを導出する、

ことを特徴とする鍵交換装置。

【請求項１０】　請求項９記載の鍵交換装置において、

前記公開鍵生成手段は、前記乱数ｋａと、前記元ｇと、前記素数ｑより、前記公開鍵ｙａをｙａ＝ｇ＾ｋａ　ｍｏｄ　ｑとして、前記有限群Ｆ上で演算し出力し、

前記共有鍵生成手段は、前記共有鍵配布先となる第２のユーザーが、前記乱数ｋｂより前記有限群Ｆ上で演算し生成した前記公開鍵ｙｂ＝ｇ＾ｋｂ　ｍｏｄ　ｑと、前記乱数ｋａにより、前記共有鍵ＫａをＫａ＝ｙｂ＾ｋａ　ｍｏｄ　ｑとして、前記有限群Ｆ上で演算し出力する、

ことを特徴とする鍵交換装置。

【請求項１１】　請求項９記載の鍵交換装置において、

前記有限群Ｆを有限体上の楕円曲線Ｅ（Ｆ）とし、前記楕円曲線Ｅ（Ｆ）の元をＧとし、

前記公開鍵生成手段は、前記乱数ｋａと、前記元Ｇと、前記素数ｑより、前記公開鍵ｙａを、ｙａ＝ｋａＧ　ｍｏｄ　ｑ

として、前記楕円曲線Ｅ（Ｆ）上で演算し出力し、

前記共有鍵生成手段は、前記共有鍵配布先となる第２のユーザーが、前記乱数ｋｂより前記楕円曲線Ｅ（Ｆ）上で演算し生成した前記公開鍵ｙｂ＝ｋｂＧ　ｍｏｄ　ｑと、前記乱数ｋａにより、前記共有鍵Ｋａを、

Ｋａ＝ｋａｙｂ　ｍｏｄ　ｑ

として、前記楕円曲線Ｅ（Ｆ）上で演算し出力する、

ことを特徴とする鍵交換装置。

【請求項１２】　請求項９ないし１１のいずれかに記載の鍵交換装置において、

前記乱数生成手段は、前記公開鍵ｙａと前記共有鍵Ｋａの演算がともに終了した後に、新たな乱数を生成する、

ことを特徴とする鍵交換装置。

【請求項１３】　乗算が定義された有限群Ｆ上の元をｇ、前記ｇの素数である位数をｑとし、０＜ｋａ＜ｑとなる乱数ｋａを生成する乱数生成手段と、

前記乱数ｋａを一時的に記憶する秘密鍵保持手段と、

前記乱数ｋａと、前記元ｇと、前記素数ｑより、公開鍵ｙａを前記有限群Ｆ上で演算し出力する公開鍵生成手段と、

共有鍵配布先となる第２のユーザーが発生した０＜ｋｂ＜ｑとなる乱数ｋｂより生成された公開鍵ｙｂと、前記秘密鍵保持手段が保持する乱数ｋａにより、共有鍵Ｋａを前記有限群Ｆ上で演算し出力する共有鍵生成手段とを備え、

少なくとも、前記乱数生成手段と、前記秘密鍵保持手段と、前記公開鍵生成手段と、前記共有鍵生成手段とが、同一の半導体集積回路上に集積され、

共有鍵配布元となる第１のユーザーの制御手段が、前記乱数生成手段と前記公開鍵生成手段とを制御して前記公開鍵ｙａを取得して、該公開鍵ｙａを前記共有

鍵配布先となる第２のユーザーへ伝送し、

前記共有鍵配布先となる第２のユーザーより前記公開鍵ｙｂを取得して、前記共有鍵生成手段を制御して前記共有鍵Ｋａを導出する、

ことを特徴とする鍵交換装置。

【請求項１４】　請求項１３記載の鍵交換装置において、

前記公開鍵生成手段は、前記乱数ｋａと、前記元ｇと、前記素数ｑより前記公開鍵ｙａを、

ｙａ＝ｇ＾ｋａ　ｍｏｄ　ｑ

として、前記有限群Ｆ上で演算し出力し、

前記共有鍵生成手段は、前記共有鍵配布先となる第２のユーザーが前記乱数ｋｂより前記有限群Ｆ上で演算し生成した前記公開鍵ｙｂ＝ｇ＾ｋｂ　ｍｏｄ　ｑと、前記秘密鍵保持手段が記憶している乱数ｋａより、前記共有鍵Ｋａを、

Ｋａ＝ｙｂ＾ｋａ　ｍｏｄ　ｑ

として、前記有限群Ｆ上で演算し出力する、

ことを特徴とする鍵交換装置。

【請求項１５】　請求項１３記載の鍵交換装置において、

前記有限群Ｆを有限体上の楕円曲線Ｅ（Ｆ）とし、前記楕円曲線Ｅ（Ｆ）の元をＧとし、前記公開鍵生成手段は、前記乱数ｋａと、前記元Ｇと、前記素数ｑより、前記公開鍵ｙａを、

ｙａ＝ｋａＧ　ｍｏｄ　ｑ

として、前記楕円曲線Ｅ（Ｆ）上で演算し出力し、

前記共有鍵生成手段は、前記共有鍵配布先となる第２のユーザーが、前記乱数ｋｂより前記楕円曲線Ｅ（Ｆ）上で演算し生成した前記公開鍵ｙｂ＝ｋｂＧ　ｍｏｄ　ｑと、前記秘密鍵保持手段が記憶している乱数ｋａにより、前記共有鍵Ｋａを、

Ｋａ＝ｋａｙｂ　ｍｏｄ　ｑ

として、前記楕円曲線Ｅ（Ｆ）上で演算し出力する、

ことを特徴とする鍵交換装置。

【請求項１６】　請求項１３ないし１５のいずれかに記載の鍵交換装置にお

いて、

前記乱数生成手段は、前記公開鍵ｙａの演算終了後に、新たな乱数を生成する、

ことを特徴とする鍵交換装置。

【請求項１７】　請求項１３ないし１５のいずれかに記載の鍵交換装置において、

前記乱数生成手段は、前記共有鍵Ｋａの演算終了後に、新たな乱数を生成し、

前記秘密鍵保持手段が、前記乱数生成手段の生成した前記新たな乱数を保持する、

ことを特徴とする鍵交換装置。

【請求項１８】　請求項９ないし１７のいずれかに記載の鍵交換装置を使用し、鍵を共有したいユーザーの双方が前記鍵を共有する、

ことを特徴とする鍵交換方法。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】

本発明は、公開されたネットワークにおける電子情報の伝送を第三者に秘匿し、安全に行うために用いられる公開鍵生成装置，共有鍵生成装置，鍵交換装置及び鍵交換方法に関し、特に第３者による装置の流用あるいは改変が極めて困難な公開鍵生成装置，共有鍵生成装置，鍵交換装置及び鍵交換方法を提供するものである。

【０００２】

【従来の技術】

従来の有限群上の離散対数問題を利用した鍵交換装置として、Diffie-Hellman鍵交換装置（以下、ＤＨ鍵交換装置と呼ぶ）が知られている（例えば、特許文献１参照）。

【０００３】

図５に、ＤＨ鍵交換装置の従来例を示す。図５において、５１は公開鍵配布元となるユーザー１の乱数生成手段、５２はユーザー１の公開鍵生成手段、５３は

ユーザー１の共有鍵生成手段である。また、５４はユーザー２の乱数生成手段、５５は公開鍵配布先となるユーザー２の公開鍵生成手段、５６はユーザー２の共有鍵生成手段である。

【０００４】

以下、図５を用いて、ユーザー１の従来のＤＨ鍵交換装置とユーザー２の従来のＤＨ鍵交換装置とで、ユーザー１とユーザー２とが鍵を共有する方法について説明する。

【０００５】

有限群Ｆ上では乗算が定義されているものとする。有限群Ｆ上の元をｇ（ｇは素数である位数ｑを持つもの）とする。また、有限群Ｆ、元ｇ、素数ｑは公開されており、少なくともユーザー１とユーザー２との間で共有されているものとする。ユーザー１とユーザー２は以下のステップを経て、鍵を共有する。

【０００６】

（ステップ１）

ユーザー１は乱数生成手段５１を用いて乱数ｋａ（０＜ｋａ＜ｑ）を生成し、これをユーザー１の秘密鍵ｋａとする。同様にユーザー２は乱数生成手段５４を用いて乱数ｋｂ（０＜ｋｂ＜ｑ）を生成し、これをユーザー２の秘密鍵ｋｂとする。

【０００７】

（ステップ２）

ユーザー１は公開鍵生成手段５２を用いて公開鍵ｙａを生成する。ここで

ｙａ＝ｇ＾ｋａ　ｍｏｄ　ｑ　　…（数１）

であり、ｙａは有限群Ｆ上で演算され求められる。ｍｏｄ　ｑはｑで割った余りを示す。同様にユーザー２は公開鍵生成手段５５を用いて公開鍵ｙｂを生成する。ここで、

ｙｂ＝ｇ＾ｋｂ　ｍｏｄ　ｑ　　…（数２）

であり、ｙｂは有限群Ｆ上で演算され求められる。

【０００８】

（ステップ３）

ユーザー１はユーザー２へ公開鍵ｙａを伝送し、ユーザー２はユーザー１へ公開鍵ｙｂを伝送する。すなわち、ユーザー１とユーザー２との間で公開鍵ｙａ、公開鍵ｙｂを交換する。

【０００９】

（ステップ４）

ユーザー１は共有鍵生成手段５３を用いて鍵Ｋａを生成する。ここで、

Ｋａ＝ｙｂ＾ｋａ　ｍｏｄ　ｑ

　＝ｇ＾（ｋａ×ｋｂ）　ｍｏｄ　ｑ　　…（数３）

であり、Ｋａは有限群Ｆ上で演算され求められる。同様にユーザー２は共有鍵生成手段５６を用いて鍵Ｋｂを生成する。ここで、

Ｋｂ＝ｙａ＾ｋｂ　ｍｏｄ　ｑ

　＝ｇ＾（ｋａ×ｋｂ）　ｍｏｄ　ｑ　　…（数４）

であり、Ｋｂは有限群Ｆ上で演算され求められる。

【００１０】

以上のステップ１～４により、ユーザー１とユーザー２との間で同一の共有鍵Ｋ＝Ｋａ＝Ｋｂが生成される。

【００１１】

上記のＤＨ鍵交換装置では、有限群Ｆにおける離散対数問題の解法の困難性に基づいて装置が構成されている。すなわちｙ＝ｇ＾ｘｍｏｄｑ（０＜ｘ＜ｑ）を満たす整数ｘをｙ、ｇより求める困難性を安全性の根拠としている。

【００１２】

有限群Ｆにおける離散対数問題の解法の困難性を根拠とする暗号系として、楕円曲線暗号系が広く知られている。すなわち、有限体上の楕円曲線をＥ（Ｆ）、楕円曲線Ｅ（Ｆ）上のあらかじめユーザー１とユーザー２との間で共有されている点をＧとし、楕円曲線Ｅ（Ｆ）上の点ｘとの演算ｘＧが定義されているものとすると、数１～数４はそれぞれ数５～数８に書き改めることができる。

【００１３】

ｙａ＝ｋａＧ　ｍｏｄ　ｑ　　…（数５）

ｙｂ＝ｋｂＧ　ｍｏｄ　ｑ　　…（数６）

Ｋａ＝ｋａ（ｙｂ）　ｍｏｄ　ｑ

　＝ｋａｋｂＧ　ｍｏｄ　ｑ　　…（数７）

Ｋｂ＝ｋｂ（ｙａ）　ｍｏｄ　ｑ

　＝ｋａｋｂＧ　ｍｏｄ　ｑ　　…（数８）

【００１４】

以上のように、楕円曲線暗号系を使用しても、ユーザー１とユーザー２との間で同一の共有鍵Ｋ＝Ｋａ＝Ｋｂが生成される。素数ｑを１６０ビット程度に選べば、現在知られている最も効率のよい計算アルゴリズムを使用し、最新のコンピュータを用いても、現実的な時間で解は求めることができないことが知られている。

【００１５】

上述したように、ＤＨ鍵交換装置ではｇ＾ｘ（楕円曲線暗号系におけるｘＧ）が鍵交換における主要な演算処理である。通常秘密鍵ｘは素数ｑと同程度のビット長（楕円曲線暗号系では１６０ビット程度）にとられるが、ユーザー１、ユーザー２以外の悪意ある第３者がｇ＾ｘ（あるいはｘＧ）を流用、あるいは鍵長をより長く改変するようなことがあれば、より強固な公開鍵暗号系を容易に構成することも可能であり、暗号系の保安上好ましくなく、特に主要な演算に高速演算アルゴリズムを使用している場合、さらに被害は甚大なものとなる。

【００１６】

【特許文献１】

特開２００１－３５２３１９号公報（第９頁、図４）

【００１７】

【発明が解決しようとする課題】

従来の公開鍵生成装置、共有鍵生成装置、鍵交換装置、及び鍵交換方法は以上のように構成されており、第３者からの攻撃に対しなんら配慮されないＤＨ鍵交換装置が用いられており、万が一主要な演算を悪意ある第３者が流用、あるいは改変することがあれば、国家の安全保障上極めて甚大な被害をもたらすという問題点を有していた。

【００１８】

本発明は以上のような問題点を解消するためになされたもので、第３者による装置の流用、あるいは改変が極めて困難な公開鍵生成装置，共有鍵生成装置，鍵交換装置、及び鍵交換方法を提供することを目的とする。

【００１９】

【課題を解決するための手段】

上記課題を解決するために、本発明（請求項１）にかかる公開鍵生成装置は、乗算が定義された有限群Ｆ上の元をｇ、前記ｇの素数である位数をｑとし、０＜ｋａ＜ｑとなる乱数ｋａを生成する乱数生成手段と、前記乱数ｋａと、前記元ｇと、前記素数ｑより、公開鍵ｙａを前記有限群Ｆ上で演算し出力する公開鍵生成手段とを備え、少なくとも前記乱数生成手段と前記公開鍵生成手段とが同一の半導体集積回路上に集積され、公開鍵配布元となる第１のユーザーの制御手段が、前記乱数生成手段と前記公開鍵生成手段とを制御して前記公開鍵ｙａを取得し、該公開鍵ｙａを公開鍵配布先となる第２のユーザーへ伝送するものである。

【００２０】

また、本発明（請求項２）にかかる公開鍵生成装置は、請求項１記載の公開鍵生成装置において、前記公開鍵生成手段は、前記乱数ｋａと、前記元ｇと、前記素数ｑより、前記公開鍵ｙａを、ｙａ＝ｇ＾ｋａ　ｍｏｄ　ｑとして、前記有限群Ｆ上で演算し出力するものである。

【００２１】

また、本発明（請求項３）にかかる公開鍵生成装置は、請求項１記載の公開鍵生成装置において、前記有限群Ｆを有限体上の楕円曲線Ｅ（Ｆ）とし、前記楕円曲線Ｅ（Ｆ）の元をＧとし、前記公開鍵生成手段が、前記乱数ｋａと、前記元Ｇと、前記素数ｑより、前記公開鍵ｙａを、ｙａ＝ｋａＧ　ｍｏｄ　ｑとして、前記楕円曲線Ｅ（Ｆ）上で演算し出力するものである。

【００２２】

また、本発明（請求項４）にかかる公開鍵生成装置は、請求項１ないし３のいずれかに記載の公開鍵生成装置において、前記乱数生成手段が、前記公開鍵ｙａの演算終了後に、新たな乱数を生成するものである。

【００２３】

また、本発明（請求項５）にかかる共有鍵生成装置は、乗算が定義された有限群Ｆ上の元をｇ、前記ｇの素数である位数をｑとし、０＜ｋａ＜ｑとなる乱数ｋａを生成する乱数生成手段と、共有鍵配布先となる第２のユーザーが発生した０＜ｋｂ＜ｑとなる乱数ｋｂより生成された公開鍵ｙｂと、前記乱数ｋａより、共有鍵Ｋａを前記有限群Ｆ上で演算し出力する共有鍵生成手段とを備え、少なくとも前記乱数生成手段と前記共有鍵生成手段とが同一の半導体集積回路上に集積され、共有鍵配布元となる第１のユーザーの制御手段が、前記共有鍵配布先となる第２のユーザーより前記公開鍵ｙｂを取得し、前記乱数生成手段と前記共有鍵生成手段とを制御して、前記共有鍵Ｋａを導出するものである。

【００２４】

また、本発明（請求項６）にかかる共有鍵生成装置は、請求項５記載の共有鍵生成装置において、前記共有鍵生成手段は、前記共有鍵配布先となる第２のユーザーが生成した前記公開鍵ｙｂ＝ｇ＾ｋｂ　ｍｏｄ　ｑと、前記乱数ｋａにより、前記共有鍵Ｋａを、Ｋａ＝ｙｂ＾ｋａ　ｍｏｄ　ｑとして、前記有限群Ｆ上で演算し出力するものである。

【００２５】

また、本発明（請求項７）にかかる共有鍵生成装置は、請求項５記載の共有鍵生成装置において、前記有限群Ｆを有限体上の楕円曲線Ｅ（Ｆ）とし、前記楕円曲線Ｅ（Ｆ）の元をＧとし、前記共有鍵生成手段は、前記共有鍵配布先となる第２のユーザーが前記乱数ｋｂより前記楕円曲線Ｅ（Ｆ）上で演算し生成した前記公開鍵ｙｂ＝ｋｂＧ　ｍｏｄ　ｑと、前記乱数ｋａにより、前記共有鍵Ｋａを、Ｋａ＝ｋａｙｂ　ｍｏｄ　ｑとして、前記楕円曲線Ｅ（Ｆ）上で演算し出力するものである。

【００２６】

また、本発明（請求項８）にかかる共有鍵生成装置は、請求項５ないし７のいずれかに記載の共有鍵生成装置において、前記乱数生成手段は、前記共有鍵Ｋａの演算終了後に、新たな乱数を生成するものである。

【００２７】

また、本発明（請求項９）にかかる鍵交換装置は、が定義された有限群Ｆ上の

元をｇ、前記ｇの素数である位数をｑとし、０＜ｋａ＜ｑとなる乱数ｋａを生成する乱数生成手段と、前記乱数ｋａと、前記元ｇと、前記素数ｑより、公開鍵ｙａを前記有限群Ｆ上で演算し出力する公開鍵生成手段と、共有鍵配布先となる第２のユーザーが発生した０＜ｋｂ＜ｑとなる乱数ｋｂより生成された公開鍵ｙｂと、前記乱数ｋａより、共有鍵Ｋａを前記有限群Ｆ上で演算し出力する共有鍵生成手段とを備え、少なくとも前記乱数生成手段と前記公開鍵生成手段と前記共有鍵生成手段とが同一の半導体集積回路上に集積され、共有鍵配布元となる第１のユーザーの制御手段が、前記乱数生成手段と前記公開鍵生成手段とを制御して前記公開鍵ｙｂを取得し、前記共有鍵生成手段を制御して前記共有鍵Ｋａを導出するものである。

【００２８】

また、本発明（請求項１０）にかかる鍵交換装置は、請求項９記載の鍵交換装置において、前記公開鍵生成手段は、前記乱数ｋａと、前記元ｇと、前記素数ｑより、前記公開鍵ｙａをｙａ＝ｇ＾ｋａ　ｍｏｄ　ｑとして、前記有限群Ｆ上で演算し出力し、前記共有鍵生成手段は、前記共有鍵配布先となる第２のユーザーが、前記乱数ｋｂより前記有限群Ｆ上で演算し生成した前記公開鍵ｙｂ＝ｇ＾ｋｂ　ｍｏｄ　ｑと、前記乱数ｋａにより、前記共有鍵Ｋａを Ｋａ＝ｙｂ＾ｋａ　ｍｏｄ　ｑとして、前記有限群Ｆ上で演算し出力するものである。

【００２９】

また、本発明（請求項１１）にかかる鍵交換装置は、請求項９記載の鍵交換装置において、前記有限群Ｆを有限体上の楕円曲線Ｅ（Ｆ）とし、前記楕円曲線Ｅ（Ｆ）の元をＧとし、前記公開鍵生成手段は、前記乱数ｋａと、前記元Ｇと、前記素数ｑより、前記公開鍵ｙａを、ｙａ＝ｋａＧ　ｍｏｄ　ｑとして、前記楕円曲線Ｅ（Ｆ）上で演算し出力し、前記共有鍵生成手段は、前記共有鍵配布先となる第２のユーザーが、前記乱数ｋｂより前記楕円曲線Ｅ（Ｆ）上で演算し生成した前記公開鍵ｙｂ＝ｋｂＧ　ｍｏｄ　ｑと、前記乱数ｋａにより、前記共有鍵Ｋａを、Ｋａ＝ｋａｙｂ　ｍｏｄ　ｑとして、前記楕円曲線Ｅ（Ｆ）上で演算し出力するものである。

【００３０】

また、本発明（請求項１２）にかかる鍵交換装置は、請求項９ないし１１のいずれかに記載の鍵交換装置において、前記乱数生成手段は、前記公開鍵ｙａと前記共有鍵Ｋａの演算がともに終了した後に、新たな乱数を生成するものである。

【００３１】

また、本発明（請求項１３）にかかる鍵交換装置は、乗算が定義された有限群Ｆ上の元をｇ、前記ｇの素数である位数をｑとし、０＜ｋａ＜ｑとなる乱数ｋａを生成する乱数生成手段と、前記乱数ｋａを一時的に記憶する秘密鍵保持手段と、前記乱数ｋａと、前記元ｇと、前記素数ｑより、公開鍵ｙａを前記有限群Ｆ上で演算し出力する公開鍵生成手段と、共有鍵配布先となる第２のユーザーが発生した０＜ｋｂ＜ｑとなる乱数ｋｂより生成された公開鍵ｙｂと、前記秘密鍵保持手段が保持する乱数ｋａにより、共有鍵Ｋａを前記有限群Ｆ上で演算し出力する共有鍵生成手段とを備え、少なくとも、前記乱数生成手段と、前記秘密鍵保持手段と、前記公開鍵生成手段と、前記共有鍵生成手段とが、同一の半導体集積回路上に集積され、共有鍵配布元となる第１のユーザーの制御手段が、前記乱数生成手段と前記公開鍵生成手段とを制御して前記公開鍵ｙａを取得して、該公開鍵ｙａを前記共有鍵配布先となる第２のユーザーへ伝送し、前記共有鍵配布先となる第２のユーザーより前記公開鍵ｙｂを取得して、前記共有鍵生成手段を制御して前記共有鍵Ｋａを導出するものである。

【００３２】

また、本発明（請求項１４）にかかる鍵交換装置は、請求項１３記載の鍵交換装置において、前記公開鍵生成手段は、前記乱数ｋａと、前記元ｇと、前記素数ｑより前記公開鍵ｙａを、ｙａ＝ｇ＾ｋａ　ｍｏｄ　ｑとして、前記有限群Ｆ上で演算し出力し、前記共有鍵生成手段は、前記共有鍵配布先となる第２のユーザーが前記乱数ｋｂより前記有限群Ｆ上で演算し生成した前記公開鍵ｙｂ＝ｇ＾ｋｂ　ｍｏｄ　ｑと、前記秘密鍵保持手段が記憶している乱数ｋａより、前記共有鍵Ｋａを、Ｋａ＝ｙｂ＾ｋａ　ｍｏｄ　ｑとして、前記有限群Ｆ上で演算し出力するものである。

【００３３】

また、本発明（請求項１５）にかかる鍵交換装置は、請求項１３記載の鍵交換

装置において、前記有限群Ｆを有限体上の楕円曲線Ｅ（Ｆ）とし、前記楕円曲線Ｅ（Ｆ）の元をＧとし、前記公開鍵生成手段は、前記乱数ｋａと、前記元Ｇと、前記素数ｑより、前記公開鍵ｙａを、ｙａ＝ｋａＧ　ｍｏｄ　ｑとして、前記楕円曲線Ｅ（Ｆ）上で演算し出力し、前記共有鍵生成手段は、前記共有鍵配布先となる第２のユーザーが、前記乱数ｋｂより前記楕円曲線Ｅ（Ｆ）上で演算し生成した前記公開鍵ｙｂ＝ｋｂＧ　ｍｏｄ　ｑと、前記秘密鍵保持手段が記憶している乱数ｋａにより、前記共有鍵Ｋａを、Ｋａ＝ｋａｙｂ　ｍｏｄ　ｑとして、前記楕円曲線Ｅ（Ｆ）上で演算し出力するものである。

【００３４】

また、本発明（請求項１６）にかかる鍵交換装置は、請求項１３ないし１５のいずれかに記載の鍵交換装置において、前記乱数生成手段は、前記公開鍵ｙａの演算終了後に、新たな乱数を生成するものである。

【００３５】

また、本発明（請求項１７）にかかる鍵交換装置は、請求項１３ないし１５のいずれかに記載の鍵交換装置において、前記乱数生成手段は、前記共有鍵Ｋａの演算終了後に、新たな乱数を生成し、前記秘密鍵保持手段が、前記乱数生成手段の生成した前記新たな乱数を保持するものである。

【００３６】

また、本発明（請求項１８）にかかる鍵交換装置は、請求項９ないし１７のいずれかに記載の鍵交換装置を使用し、鍵を共有したいユーザーの双方が前記鍵を共有するものである。

【００３７】

【発明の実施の形態】

以下、本発明の実施の形態について、図面を用いて説明する。

【００３８】

（実施の形態１）

図１は、本発明の請求項１に対応する実施の形態１による公開鍵生成装置のブロック構成図を示すものである。

【００３９】

図１において、１１は乱数生成手段、１２は公開鍵生成手段、１３は１つのパッケージに収められた半導体集積回路（以下ＬＳＩと呼ぶ）、１４は半導体集積回路（ＬＳＩ）１３を制御する制御手段、１５は半導体集積回路１３、制御手段１４を含む公開鍵配布元であるユーザー１の公開鍵生成装置である。

【００４０】

以下、図１を参照しながら、本実施の形態１の公開鍵生成装置の動作について説明する。

乱数生成手段１１は、制御手段１４によって制御され、乱数ｋａを生成し、これを秘密鍵ｋａとする。ここで秘密鍵ｋａは、乗算が定義された有限群Ｆ上の元をｇ、前記ｇの素数である位数をｑとした時、０＜ｋａ＜ｑを満たしている。制御手段１４は、乱数を生成するタイミングや乱数の種、初期値の設定を行う。制御手段１４には、例えばマイクロコンピュータが使用される。

【００４１】

公開鍵生成手段１２は、上記制御手段１４により制御され、公開鍵ｙａを生成する。公開鍵ｙａは、上述した数１式に基づいて秘密鍵ｋａより求められる。生成された公開鍵ｙａは、制御手段１４によって公開鍵配布先であるユーザー２へ伝送される。

【００４２】

少なくとも乱数生成手段１１と、公開鍵生成手段１２を、ＬＳＩ１３内部に集積すれば、上記数１式の演算を他の暗号処理へ流用、あるいは改変することは非常に困難である。加えて制御手段１４を集積すれば、さらに効果が高まる。また公開鍵ｙａ生成後、乱数生成手段１１が、新たに乱数を生成するようにすれば、公開鍵ｙａは出力される毎に異なる値をとる。この時、上記数１式から明らかなように、公開鍵ｙａは、乱数の関数となる。よって、ユーザー１を含めた誰もが、本公開鍵生成装置１５を公開鍵ｙａの生成以外に流用、あるいは改変することは極めて困難である。

【００４３】

以上のように、本実施の形態１による公開鍵生成装置によれば、公開鍵生成装置１５を、乱数生成手段１１と公開鍵生成手段１２とを１つのＬＳＩ１５に集積

化して構成するようにしたので、従来、何ら安全対策のなされていない演算アルゴリズムを用いて秘密鍵及び共有鍵を作製する場合に比べて、秘密鍵ｋａは、チップ内部で公開鍵ｙａの生成にのみ用いられる構成となり、公開鍵生成装置１５の数１式の演算が外部には漏れることがなく、このようなＬＳＩ１３を用いることで、本公開鍵生成装置１５を公開鍵ｙａの生成以外に流用、あるいは改変することが極めて困難な状態となり、第３者の不正な攻撃に対する強度が極めて高い。

【００４４】

なお、数１式に基づいて公開鍵ｙａを演算する例について説明したが、楕円曲線暗号を使用し、数５式に基づいて公開鍵ｙａを演算するようにしても、同様の効果が得られる。

【００４５】

また、離散対数問題に基づく公開鍵暗号系を使用すれば、どのような公開鍵暗号系に対しても同様の効果が得られることは言うまでもない。

【００４６】

（実施の形態２）

次に、本発明の請求項５に対応する実施の形態２による共有鍵生成装置について説明する。

図２は、本発明の実施の形態２による共有鍵生成装置のブロック構成図を示すものである。図２において、図１と同一符号は同一、または相当部分を示し、２１は共有鍵生成手段、２２は乱数生成手段１１と上記共有鍵生成手段２１とを含むＬＳＩ、２３はＬＳＩ２２を制御する制御手段、２４は共有鍵配布先となるユーザー２が生成した公開鍵を元に共有鍵を作成する、共有鍵配布元であるユーザー１の共有鍵生成装置を示す。以下、図２を参照しながら、本実施の形態２の共有鍵生成装置２４の動作について説明する。

【００４７】

乱数生成手段１１は制御手段２３に制御され、乱数ｋａを生成し、これを秘密鍵ｋａとする。ここで秘密鍵ｋａは、乗算が定義された有限群Ｆ上の元をｇ、前記ｇの素数である位数をｑとした時、０＜ｋａ＜ｑを満たしている。制御手段２

３は乱数を生成するタイミングや乱数の種、初期値の設定を行う。制御手段２３には、例えばマイクロコンピュータが使用される。さらに制御手段２３は、共有鍵配布先となるユーザー２より数２式で表されるユーザー２の公開鍵ｙｂを取得する。共有鍵生成手段２１は制御手段２３に制御され、共有鍵Ｋａを生成する。共有鍵Ｋａは数３式に基づいてユーザー１の秘密鍵ｋａとユーザー２の公開鍵ｙｂとにより演算される。生成された共有鍵Ｋａは、例えば、制御手段１４によって秘密鍵暗号方式の鍵として用いられ、ユーザー１とユーザー２との間でこの共通の共有鍵Ｋａを用いた暗号化伝送に使用される。

【００４８】

以上の構成において、少なくとも乱数生成手段１１と共有鍵生成手段２１とをＬＳＩ２２内部に集積すれば、数３式の演算を他の暗号処理へ流用あるいは改変することは非常に困難である。加えて制御手段２３を集積すれば、さらに効果が高まる。また共有鍵Ｋａ生成後、乱数生成手段１１が新たに乱数を生成するようにすれば、共有鍵Ｋａは出力される毎に異なる値をとる。この時、数３式から明らかなように、共有鍵Ｋａは乱数の関数となる。よって、ユーザー１を含めた誰もが本共有鍵生成装置２４を共有鍵Ｋａの生成以外に流用あるいは改変することは極めて困難である。

【００４９】

以上のように、本実施の形態２による共有鍵生成装置によれば、共有鍵生成装置２４を、乱数生成手段１１と共有鍵生成手段２１とを１つのＬＳＩ２２に集積化して構成するようにしたので、秘密鍵ｋａはチップ内部で共有鍵Ｋａの生成にのみ用いられる構成となり、共有鍵生成装置２４の数３式の演算が外部には漏れることがなく、このようなＬＳＩ２２を用いることで、本共有鍵生成装置２４を共有鍵Ｋａの生成以外に流用あるいは改変することが極めて困難な状態となり、第３者の不正な攻撃に対する強度が極めて高い。

【００５０】

なお、数３式に基づいて共有鍵Ｋａを演算する例について説明したが、楕円曲線暗号を使用し、数７式に基づいて共有鍵Ｋａを演算しても同様の効果が得られる。

また、離散対数問題に基づく公開鍵暗号系を使用すれば、どのような公開鍵暗号系に対しても同様の効果が得られることは言うまでもない。

【００５１】

（実施の形態３）

次に、本発明の請求項９に対応する実施の形態３による鍵交換装置について説明する。

図３は、本発明の実施の形態３である鍵交換装置のブロック構成図を示すものである。

【００５２】

図３において、図１または図２と同一符号は同一、または相当部分を示し、３１は乱数生成手段１１，公開鍵生成手段１２，共有鍵生成手段２１とを含むＬＳＩ、３２はＬＳＩ３１を制御する制御手段、３３は公開鍵配布元、及び共有鍵配布先となるユーザー２の生成した公開鍵を基に作成した共有鍵の配布元、となるユーザー１の鍵交換装置である。

【００５３】

以下、図３を参照しながら、実施の形態３の鍵交換装置の動作について説明する。

乱数生成手段１１は制御手段３２に制御され、乱数ｋａを生成し、これを秘密鍵ｋａとする。ここで秘密鍵ｋａは、乗算が定義された有限群Ｆ上の元をｇ、前記ｇの素数である位数をｑとした時、０＜ｋａ＜ｑを満たしている。制御手段３２は乱数を生成するタイミングや乱数の種、初期値の設定を行う。制御手段３２には、例えばマイクロコンピュータが使用される。公開鍵生成手段１２は制御手段３２に制御され、公開鍵ｙａを生成する。公開鍵ｙａは数１式に基づいて演算される。生成された公開鍵ｙａは、制御手段３２によってユーザー２へ伝送される。

【００５４】

さらに制御手段３２は、ユーザー２より数２式で表されるユーザー２の公開鍵ｙｂを取得する。共有鍵生成手段２１は制御手段３２に制御され、共有鍵Ｋａを生成する。共有鍵Ｋａは数３式に基づいて秘密鍵ｋａと公開鍵ｙｂより演算され

る。生成された共有鍵Ｋａは、制御手段３２によって例えば秘密鍵暗号方式の鍵として用いられ、ユーザー１とユーザー２との間の暗号化伝送に使用される。

【００５５】

少なくとも乱数生成手段１１と公開鍵生成手段１２と共有鍵生成手段２１をＬＳＩ３１内部に集積すれば、数１式および数３式の演算を他の暗号処理へ流用あるいは改変することは非常に困難である。加えて制御手段３２を集積すれば、さらに効果が高まる。また公開鍵ｙａと共有鍵Ｋａとを生成後、乱数生成手段１１が新たに乱数を生成するようにすれば、数１式および数３式から明らかなように、公開鍵ｙａと共有鍵Ｋａは乱数の関数となる。よって、ユーザー１を含めた誰もが本鍵交換装置３３を鍵交換処理以外に流用あるいは改変することは極めて困難である。

【００５６】

以上のように、本実施の形態３による鍵交換装置によれば、鍵交換装置３３を、乱数生成手段１１と公開鍵生成手段１２と共有鍵生成手段２１とを、１つのＬＳＩ１３１に集積化して構成するようにしたので、秘密鍵ｋａはチップ内部で公開鍵ｙａ、及び共有鍵Ｋａの生成にのみ用いられる構成となり、鍵交換装置３３の数１式及び数３式の演算が外部には漏れることがなく、このようなＬＳＩ１３１を用いることで本鍵交換装置３３を鍵交換以外の暗号化処理に流用あるいは改変することが極めて困難となり、第３者の不正な攻撃に対する強度が極めて高い。

【００５７】

なお、数１式および数３式に基づいて公開鍵ｙａと共有鍵Ｋａを演算する例について説明したが、楕円曲線暗号を使用し、数５式および数７式に基づいて公開鍵ｙａと共有鍵Ｋａとを演算しても同様の効果が得られる。

【００５８】

また、離散対数問題に基づく公開鍵暗号系を使用すれば、どのような公開鍵暗号系に対しても同様の効果が得られることは言うまでもない。

なお、本実施の形態３における鍵交換装置３３と同様の構成をもつ鍵交換装置をユーザー２が使用することによって、ユーザー１とユーザー２の間の鍵交換処

理を極めて安全に行うことができることは説明するまでもない。

【００５９】

（実施の形態４）

次に、本発明の請求項１３に対応する実施の形態４による鍵交換装置について説明する。

図４は、本発明の実施の形態４による鍵交換装置のブロック構成図を示すものである。

【００６０】

図４において、図１または図２と同一符号は同一、または相当部分を示し、４１は秘密鍵保持手段、４２は乱数生成手段１１，公開鍵生成手段，共有鍵生成手段２１，秘密鍵保持手段４１とを含むＬＳＩ、４３はＬＳＩ４２を制御する制御手段、４４は公開鍵配布元、及び共有鍵配布先となるユーザー２の生成した公開鍵を基に作成した共有鍵の配布元、となるユーザー１の鍵交換装置である。以下、図４を参照しながら、本実施の形態４の鍵交換装置の動作について説明する。

【００６１】

乱数生成手段１１は制御手段４３に制御され、乱数ｋａを生成し、これを秘密鍵ｋａとする。ここで秘密鍵ｋａは、乗算が定義された有限群Ｆ上の元をｇ、前記ｇの素数である位数をｑとした時、０＜ｋａ＜ｑを満たしている。制御手段４３は乱数を生成するタイミングや乱数の種、初期値の設定を行う。制御手段４３には、例えばマイクロコンピュータが使用される。秘密鍵保持手段４１は秘密鍵ｋａを一時的に記憶する。公開鍵生成手段１２は制御手段４３に制御され、公開鍵ｙａを生成する。公開鍵ｙａは数１式に基づいて演算される。生成された公開鍵ｙａは、制御手段４３によってユーザー２へ伝送される。

【００６２】

さらに制御手段４３は、ユーザー２より数２式で表されるユーザー２の公開鍵ｙｂを取得する。共有鍵生成手段２１は制御手段４３に制御され、共有鍵Ｋａを生成する。共有鍵Ｋａは数３式に基づいて秘密鍵保持手段４１が記憶している秘密鍵ｋａと公開鍵ｙｂとより演算される。生成された共有鍵Ｋａは、制御手段４３によって、例えば秘密鍵暗号方式の鍵として用いられ、ユーザー１とユーザー

２との間の暗号化伝送に使用される。

【００６３】

少なくとも乱数生成手段１１と公開鍵生成手段１２と共有鍵生成手段２１と秘密鍵保持手段４１とをＬＳＩ４２内部に集積すれば、数１式および数３式の演算を他の暗号処理へ流用あるいは改変することは非常に困難である。加えて制御手段４３を集積すれば、さらに効果が高まる。

【００６４】

また公開鍵ｙａを生成後、乱数生成手段１１が新たに乱数を生成するようにすれば、公開鍵ｙａは出力される毎に異なる値をとる。この時、数１式から明らかなように、公開鍵ｙａは乱数の関数となる。共有鍵生成手段２１が共有鍵Ｋａを生成する以前に、乱数生成手段１１が新たに乱数を生成しても、秘密鍵保持手段４１が秘密鍵ｋａを保持しているため、共有鍵生成手段２１は正しく共有鍵Ｋａを生成することができる。

【００６５】

加えて、共有鍵生成手段２１により共有鍵Ｋａを生成した後、乱数生成手段１１が新たに乱数を生成し、生成した乱数を秘密鍵保持手段４１が保持するようにすれば、共有鍵Ｋａは出力される毎に異なる値をとる。この時、数３式から明らかなように、共有鍵Ｋａは乱数の関数となる。

【００６６】

よって、ユーザー１を含めた誰もが本鍵交換装置を鍵交換処理以外に流用あるいは改変することは極めて困難である。またＬＳＩ４２の外部に出力される公開鍵ｙａ、共有鍵Ｋａを観測しても乱数の関数となっているため、公開鍵生成手段１２と共有鍵生成手段２１の構成を類推することすら不可能である。

【００６７】

以上のように、本実施の形態４による鍵交換装置によれば、鍵交換装置４４を、乱数生成手段１１と公開鍵生成手段１２と共有鍵生成手段２１と秘密鍵保持手段４１とを１つのＬＳＩ４２に集積化して構成するようにしたので、秘密鍵ｋａはチップ内部で公開鍵ｙａ、及び共有鍵Ｋａの生成にのみ用いられる構成となり、鍵交換装置４４の数１式及び数３式の演算が外部には漏れることがなく、この

ようなＬＳＩ４２を用いることで本鍵交換装置４４を鍵交換以外の暗号化処理に流用あるいは改変することが極めて困難となり、第３者の不正な攻撃に対する強度が極めて高い。

【００６８】

加えて、共有鍵生成手段２１が共有鍵Ｋａを生成する以前に、乱数生成手段１１が新たに乱数を生成しても、共有鍵生成手段２１が正しく共有鍵Ｋａを生成することができる。

【００６９】

なお、数１式および数３式に基づいて公開鍵ｙａと共有鍵Ｋａを演算する例について説明したが、楕円曲線暗号を使用し、数５式および数７式に基づいて公開鍵ｙａと共有鍵Ｋａを演算しても同様の効果が得られる。

【００７０】

また、離散対数問題に基づく公開鍵暗号系を使用すれば、どのような公開鍵暗号系に対しても同様の効果が得られることは言うまでもない。

【００７１】

なお、本実施の形態４における鍵交換装置４４と同様の構成をもつ鍵交換装置をユーザー２が使用することによって、ユーザー１とユーザー２の間の鍵交換処理を極めて安全に行うことができることは説明するまでもない。

【００７２】

【発明の効果】

以上のように、本発明の請求項１にかかる公開鍵生成装置によれば、乗算が定義された有限群Ｆ上の元をｇ、前記ｇの素数である位数をｑとし、０＜ｋａ＜ｑとなる乱数ｋａを生成する乱数生成手段と、前記乱数ｋａと、前記元ｇと、前記素数ｑより、公開鍵ｙａを前記有限群Ｆ上で演算し出力する公開鍵生成手段とを備え、少なくとも前記乱数生成手段と前記公開鍵生成手段とが同一の半導体集積回路上に集積され、公開鍵配布元となる第１のユーザーの制御手段が、前記乱数生成手段と前記公開鍵生成手段とを制御して前記公開鍵ｙａを取得し、該公開鍵ｙａを公開鍵配布先となる第２のユーザーへ伝送するものとしたので、秘密鍵ｋａは半導体集積回路のチップ内部で公開鍵ｙａの生成にのみ用いられる構成とな

り、鍵交換装置の演算が外部には漏れることがなく、このような集積回路を用いることで本公開鍵生成装置を公開鍵ｙａの生成以外に流用あるいは改変することが極めて困難な状態となり、第３者の不正な攻撃に対する強度を極めて高いものとすることができるという効果が得られる。

【００７３】

また、本発明の請求項２にかかる公開鍵生成装置によれば、請求項１記載の公開鍵生成装置において、前記公開鍵生成手段は、前記乱数ｋａと、前記元ｇと、前記素数ｑより、前記公開鍵ｙａを、ｙａ＝ｇ＾ｋａ　ｍｏｄ　ｑとして、前記有限群Ｆ上で演算し出力するものとしたので、有限群Ｆにおける離散対数問題の解法の困難性を根拠とした暗号系において、公開鍵生成装置を公開鍵ｙａの生成以外に流用あるいは改変することが極めて困難な状態となり、第３者の不正な攻撃に対する強度を極めて高いものとすることができるという効果が得られる。

【００７４】

また、本発明の請求項３にかかる公開鍵生成装置によれば、請求項１記載の公開鍵生成装置において、前記有限群Ｆを有限体上の楕円曲線Ｅ（Ｆ）とし、前記楕円曲線Ｅ（Ｆ）の元をＧとし、前記公開鍵生成手段が、前記乱数ｋａと、前記元Ｇと、前記素数ｑより、前記公開鍵ｙａを、ｙａ＝ｋａＧ　ｍｏｄ　ｑとして、前記楕円曲線Ｅ（Ｆ）上で演算し出力するものとしたので、楕円曲線暗号系においても、公開鍵生成装置を公開鍵ｙａの生成以外に流用あるいは改変することが極めて困難な状態となり、第３者の不正な攻撃に対する強度を極めて高いものとすることができるという効果が得られる。

【００７５】

また、本発明の請求項４にかかる公開鍵生成装置によれば、請求項１ないし３のいずれかに記載の公開鍵生成装置において、前記乱数生成手段が、前記公開鍵ｙａの演算終了後に、新たな乱数を生成するものとしたので、公開鍵ｙａは出力される毎に異なるものとなり、第３者の不正な攻撃に対する強度をさらに高いものとすることができるという効果が得られる。

【００７６】

また、本発明の請求項５にかかる共有鍵生成装置は、乗算が定義された有限群

Ｆ上の元をｇ、前記ｇの素数である位数をｑとし、０＜ｋａ＜ｑとなる乱数ｋａを生成する乱数生成手段と、共有鍵配布先となる第２のユーザーが発生した０＜ｋｂ＜ｑとなる乱数ｋｂより生成された公開鍵ｙｂと、前記乱数ｋａより、共有鍵Ｋａを前記有限群Ｆ上で演算し出力する共有鍵生成手段とを備え、少なくとも前記乱数生成手段と前記共有鍵生成手段とが同一の半導体集積回路上に集積され、共有鍵配布元となる第１のユーザーの制御手段が、前記共有鍵配布先となる第２のユーザーより前記公開鍵ｙｂを取得し、前記乱数生成手段と前記共有鍵生成手段とを制御して、前記共有鍵Ｋａを導出するものとしたので、秘密鍵ｋａは半導体集積回路のチップ内部で共有鍵Ｋａの生成にのみ用いられる構成となり、鍵交換装置の演算が外部には漏れることがなく、このような集積回路を用いることで本共有鍵生成装置を共有鍵Ｋａの生成以外に流用あるいは改変することが極めて困難な状態となり、第３者の不正な攻撃に対する強度を極めて高いものとすることができるという効果が得られる。

【００７７】

また、本発明の請求項６にかかる共有鍵生成装置は、請求項５記載の共有鍵生成装置において、前記共有鍵生成手段は、前記共有鍵配布先となる第２のユーザーが生成した前記公開鍵ｙｂ＝ｇ＾ｋｂ　ｍｏｄ　ｑと、前記乱数ｋａにより、前記共有鍵Ｋａを、Ｋａ＝ｙｂ＾ｋａ　ｍｏｄ　ｑとして、前記有限群Ｆ上で演算し出力するものとしたので、有限群Ｆにおける離散対数問題の解法の困難性を根拠とした暗号系において、共有鍵生成装置を共有鍵Ｋａの生成以外に流用あるいは改変することが極めて困難な状態となり、第３者の不正な攻撃に対する強度を極めて高いものとすることができるという効果が得られる。

【００７８】

また、本発明の請求項７にかかる共有鍵生成装置は、請求項５記載の共有鍵生成装置において、前記有限群Ｆを有限体上の楕円曲線Ｅ（Ｆ）とし、前記楕円曲線Ｅ（Ｆ）の元をＧとし、前記共有鍵生成手段は、前記共有鍵配布先となる第２のユーザーが前記乱数ｋｂより前記楕円曲線Ｅ（Ｆ）上で演算し生成した前記公開鍵ｙｂ＝ｋｂＧ　ｍｏｄ　ｑと、前記乱数ｋａにより、前記共有鍵Ｋａを、Ｋａ＝ｋａｙｂ　ｍｏｄ　ｑとして、前記楕円曲線Ｅ（Ｆ）上で演算し出力するも

のとしたので、楕円曲線暗号系においても、共有鍵生成装置を共有鍵Ｋａの生成以外に流用あるいは改変することが極めて困難な状態となり、第３者の不正な攻撃に対する強度を極めて高いものとすることができるという効果が得られる。

【００７９】

また、本発明の請求項８にかかる共有鍵生成装置は、請求項５ないし７のいずれかに記載の共有鍵生成装置において、前記乱数生成手段は、前記共有鍵Ｋａの演算終了後に、新たな乱数を生成するものとしたので、共有鍵Ｋａは出力される毎に異なるものとなり、第３者の不正な攻撃に対する強度をさらに高いものとすることができるという効果が得られる。

【００８０】

また、本発明の請求項９にかかる鍵交換装置は、乗算が定義された有限群Ｆ上の元をｇ、前記ｇの素数である位数をｑとし、０＜ｋａ＜ｑとなる乱数ｋａを生成する乱数生成手段と、前記乱数ｋａと、前記元ｇと、前記素数ｑより、公開鍵ｙａを前記有限群Ｆ上で演算し出力する公開鍵生成手段と、共有鍵配布先となる第２のユーザーが発生した０＜ｋｂ＜ｑとなる乱数ｋｂより生成された公開鍵ｙｂと、前記乱数ｋａより、共有鍵Ｋａを前記有限群Ｆ上で演算し出力する共有鍵生成手段とを備え、少なくとも前記乱数生成手段と前記公開鍵生成手段と前記共有鍵生成手段とが同一の半導体集積回路上に集積され、共有鍵配布元となる第１のユーザーの制御手段が、前記乱数生成手段と前記公開鍵生成手段とを制御して前記公開鍵ｙｂを取得し、前記共有鍵生成手段を制御して前記共有鍵Ｋａを導出するものとしたので、秘密鍵ｋａは半導体集積回路のチップ内部で公開鍵ｙａ、及び共有鍵Ｋａの生成にのみ用いられる構成となり、鍵交換装置の演算が外部には漏れることがなく、このような集積回路を用いることで本鍵交換装置を鍵交換以外の暗号化処理に流用あるいは改変することが極めて困難となり、第３者の不正な攻撃に対する強度が極めて高いものとすることができるという効果が得られる。

【００８１】

また、本発明の請求項１０にかかる鍵交換装置は、請求項９記載の鍵交換装置において、前記公開鍵生成手段は、前記乱数ｋａと、前記元ｇと、前記素数ｑよ

り、前記公開鍵ｙａをｙａ＝ｇ＾ｋａ　ｍｏｄ　ｑとして、前記有限群Ｆ上で演算し出力し、前記共有鍵生成手段は、前記共有鍵配布先となる第２のユーザーが、前記乱数ｋｂより前記有限群Ｆ上で演算し生成した前記公開鍵ｙｂ＝ｇ＾ｋｂ　ｍｏｄ　ｑと、前記乱数ｋａにより、前記共有鍵ＫａをＫａ＝ｙｂ＾ｋａ　ｍｏｄ　ｑとして、前記有限群Ｆ上で演算し出力するものとしたので、有限群Ｆにおける離散対数問題の解法の困難性を根拠とした暗号系において、鍵交換装置を鍵交換以外の暗号化処理に流用あるいは改変することが極めて困難な状態となり、第３者の不正な攻撃に対する強度を極めて高いものとすることができるという効果が得られる。

【００８２】

また、本発明の請求項１１にかかる鍵交換装置は、請求項９記載の鍵交換装置において、前記有限群Ｆを有限体上の楕円曲線Ｅ（Ｆ）とし、前記楕円曲線Ｅ（Ｆ）の元をＧとし、前記公開鍵生成手段は、前記乱数ｋａと、前記元Ｇと、前記素数ｑより、前記公開鍵ｙａを、ｙａ＝ｋａＧ　ｍｏｄ　ｑとして、前記楕円曲線Ｅ（Ｆ）上で演算し出力し、前記共有鍵生成手段は、前記共有鍵配布先となる前記第２のユーザーが、前記乱数ｋｂより前記楕円曲線Ｅ（Ｆ）上で演算し生成した前記公開鍵ｙｂ＝ｋｂＧ　ｍｏｄ　ｑと、前記乱数ｋａにより、前記共有鍵Ｋａを、Ｋａ＝ｋａｙｂ　ｍｏｄ　ｑとして、前記楕円曲線Ｅ（Ｆ）上で演算し出力するものとしたので、楕円曲線暗号系においても、鍵交換装置を鍵交換以外の暗号化処理に流用あるいは改変することが極めて困難な状態となり、第３者の不正な攻撃に対する強度を極めて高いものとすることができるという効果が得られる。

【００８３】

また、本発明の請求項１２にかかる鍵交換装置は、請求項９ないし１１のいずれかに記載の鍵交換装置において、前記乱数生成手段は、前記公開鍵ｙａと前記共有鍵Ｋａの演算がともに終了した後に、新たな乱数を生成するものとしたので、公開鍵ｙａ、及び共有鍵Ｋａは出力される毎に異なるものとなり、第３者の不正な攻撃に対する強度をさらに高いものとすることができるという効果が得られる。

【００８４】

また、本発明の請求項１３にかかる鍵交換装置は、乗算が定義された有限群Ｆ上の元をｇ、前記ｇの素数である位数をｑとし、０＜ｋａ＜ｑとなる乱数ｋａを生成する乱数生成手段と、前記乱数ｋａを一時的に記憶する秘密鍵保持手段と、前記乱数ｋａと、前記元ｇと、前記素数ｑより、公開鍵ｙａを前記有限群Ｆ上で演算し出力する公開鍵生成手段と、共有鍵配布先となる第２のユーザーが発生した０＜ｋｂ＜ｑとなる乱数ｋｂより生成された公開鍵ｙｂと、前記秘密鍵保持手段が保持する乱数ｋａにより、共有鍵Ｋａを前記有限群Ｆ上で演算し出力する共有鍵生成手段とを備え、少なくとも、前記乱数生成手段と、前記秘密鍵保持手段と、前記公開鍵生成手段と、前記共有鍵生成手段とが、同一の半導体集積回路上に集積され、共有鍵配布元となる第１のユーザーの制御手段が、前記乱数生成手段と前記公開鍵生成手段とを制御して前記公開鍵ｙａを取得して、該公開鍵ｙａを前記共有鍵配布先となる第２のユーザーへ伝送し、前記共有鍵配布先となる第２のユーザーより前記公開鍵ｙｂを取得して、前記共有鍵生成手段を制御して前記共有鍵Ｋａを導出するものとしたので、秘密鍵ｋａは半導体集積回路のチップ内部で公開鍵ｙａ、及び共有鍵Ｋａの生成にのみ用いられる構成となり、鍵交換装置の演算が外部には漏れることがなく、このような集積回路を用いることで本鍵交換装置を鍵交換以外の暗号化処理に流用あるいは改変することが極めて困難となり、第３者の不正な攻撃に対する強度が極めて高いものとすることができるという効果が得られるのに加えて、共有鍵生成手段が共有鍵Ｋａを生成する以前に、乱数生成手段が新たに乱数を生成しても、共有鍵生成手段は正しく共有鍵Ｋａを生成することができるという効果が得られる。

【００８５】

また、本発明の請求項１４にかかる鍵交換装置は、請求項１３記載の鍵交換装置において、前記公開鍵生成手段は、前記乱数ｋａと前記元ｇと前記素数ｑより前記公開鍵ｙａを、ｙａ＝ｇ＾ｋａ　ｍｏｄ　ｑとして、前記有限群Ｆ上で演算し出力し、前記共有鍵生成手段は、前記共有鍵配布先となる第２のユーザーが前記乱数ｋｂより前記有限群Ｆ上で演算し生成した前記公開鍵ｙｂ＝ｇ＾ｋｂ　ｍｏｄ　ｑと前記秘密鍵保持手段が記憶している乱数ｋａより前記共有鍵Ｋａを、

Ｋａ＝ｙｂ＾ｋａ　ｍｏｄ　ｑとして、前記有限群Ｆ上で演算し出力するものとしたので、有限群Ｆにおける離散対数問題の解法の困難性を根拠とした暗号系において、鍵交換装置を鍵交換以外の暗号化処理に流用あるいは改変することが極めて困難な状態となり、第３者の不正な攻撃に対する強度を極めて高いものとすることができるという効果が得られる。

【００８６】

また、本発明の請求項１５にかかる鍵交換装置は、請求項１３記載の鍵交換装置において、前記有限群Ｆを有限体上の楕円曲線Ｅ（Ｆ）とし、前記楕円曲線Ｅ（Ｆ）の元をＧとし、前記公開鍵生成手段は、前記乱数ｋａと、前記元Ｇと、前記素数ｑより、前記公開鍵ｙａを、ｙａ＝ｋａＧ　ｍｏｄ　ｑとして、前記楕円曲線Ｅ（Ｆ）上で演算し出力し、前記共有鍵生成手段は、前記共有鍵配布先となる第２のユーザーが、前記乱数ｋｂより前記楕円曲線Ｅ（Ｆ）上で演算し生成した前記公開鍵ｙｂ＝ｋｂＧ　ｍｏｄ　ｑと、前記秘密鍵保持手段が記憶している乱数ｋａにより、前記共有鍵Ｋａを、Ｋａ＝ｋａｙｂ　ｍｏｄ　ｑとして、前記楕円曲線Ｅ（Ｆ）上で演算し出力するものとしたので、楕円曲線暗号系においても、鍵交換装置を鍵交換以外の暗号化処理に流用あるいは改変することが極めて困難な状態となり、第３者の不正な攻撃に対する強度を極めて高いものとすることができるという効果が得られる。

【００８７】

また、本発明の請求項１６にかかる鍵交換装置は、請求項１３ないし１５のいずれかに記載の鍵交換装置において、前記乱数生成手段は、前記公開鍵ｙａの演算終了後に、新たな乱数を生成するようにしたので、公開鍵ｙａ、及び共有鍵Ｋａは出力される毎に異なるものとなり、第３者の不正な攻撃に対する強度をさらに高いものとすることができるという効果が得られる。

【００８８】

また、本発明の請求項１７にかかる鍵交換装置は、請求項１３ないし１５のいずれかに記載の鍵交換装置において、

【００８９】

前記乱数生成手段は、前記共有鍵Ｋａの演算終了後に、新たな乱数を生成し、

前記秘密鍵保持手段が、前記乱数生成手段の生成した前記新たな乱数を保持するようにしたので、共有鍵生成手段が共有鍵Ｋａを生成する以前に、乱数生成手段が新たに乱数を生成しても、共有鍵生成手段が正しく共有鍵Ｋａを生成することができるという効果が得られる。

【００９０】

また、本発明の請求項１８にかかる鍵交換方法は、請求項９ないし１７のいずれかに記載の鍵交換装置を使用し、鍵を共有したいユーザーの双方が前記鍵を共有するようにしたので、鍵交換装置の演算が外部には漏れることがなく、このような集積回路を用いることで暗号鍵生成、または鍵交換以外の暗号化処理に流用あるいは改変することが極めて困難となり、第３者の不正な攻撃に対する強度が極めて高いものとすることができるという効果が得られる。

【図面の簡単な説明】

【図１】

本発明の実施の形態１における公開鍵生成装置の構成を示すブロック構成図である。

【図２】

本発明の実施の形態２における共有鍵生成装置の構成を示すブロック構成図である。

【図３】

本発明の実施の形態３における鍵交換装置の構成を示すブロック構成図である。

【図４】

本発明の実施の形態４における鍵交換装置の構成を示すブロック構成図である。

【図５】

従来の鍵交換装置の構成を示すブロック構成図である。

【符号の説明】

１１　乱数生成手段

１２　公開鍵生成手段

１３，２２，３１，４２　ＬＳＩ

１４，２３，３２，４３　制御手段

１５　公開鍵生成装置

２１　共有鍵生成手段

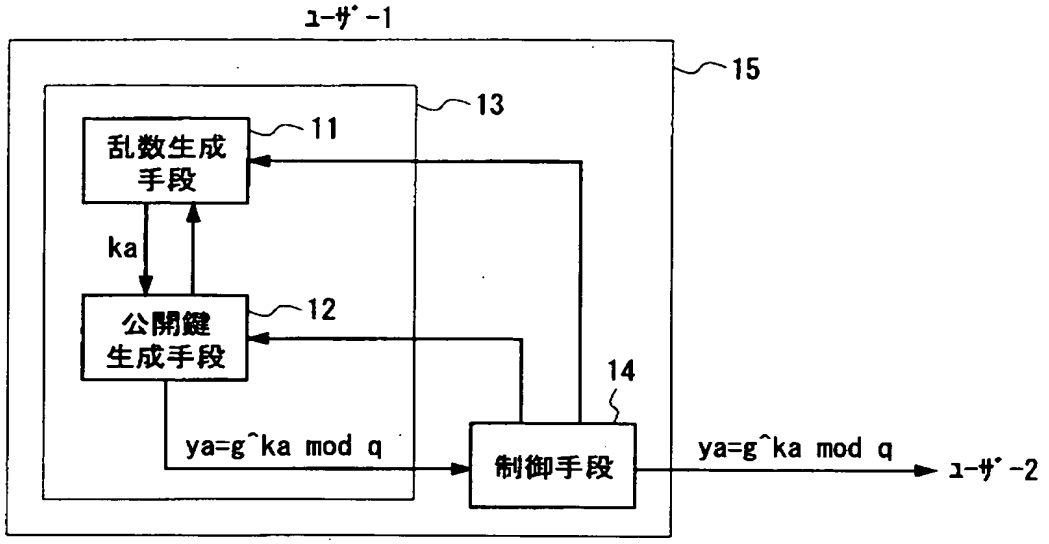
２４　共有鍵生成装置

３３，４４　鍵交換装置

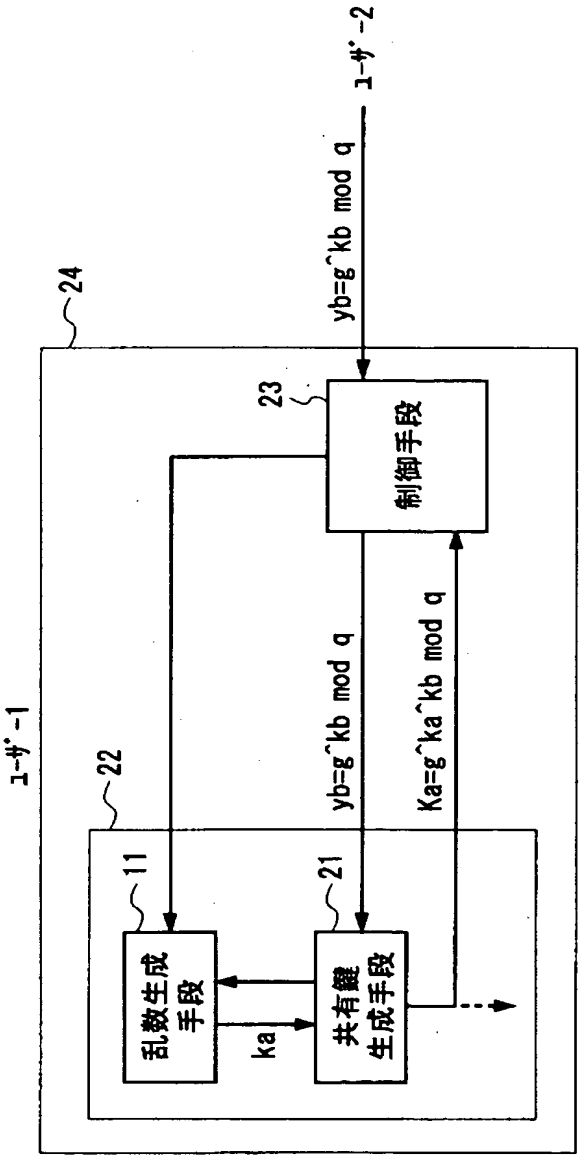
４１　秘密鍵保持手段

【書類名】　図面

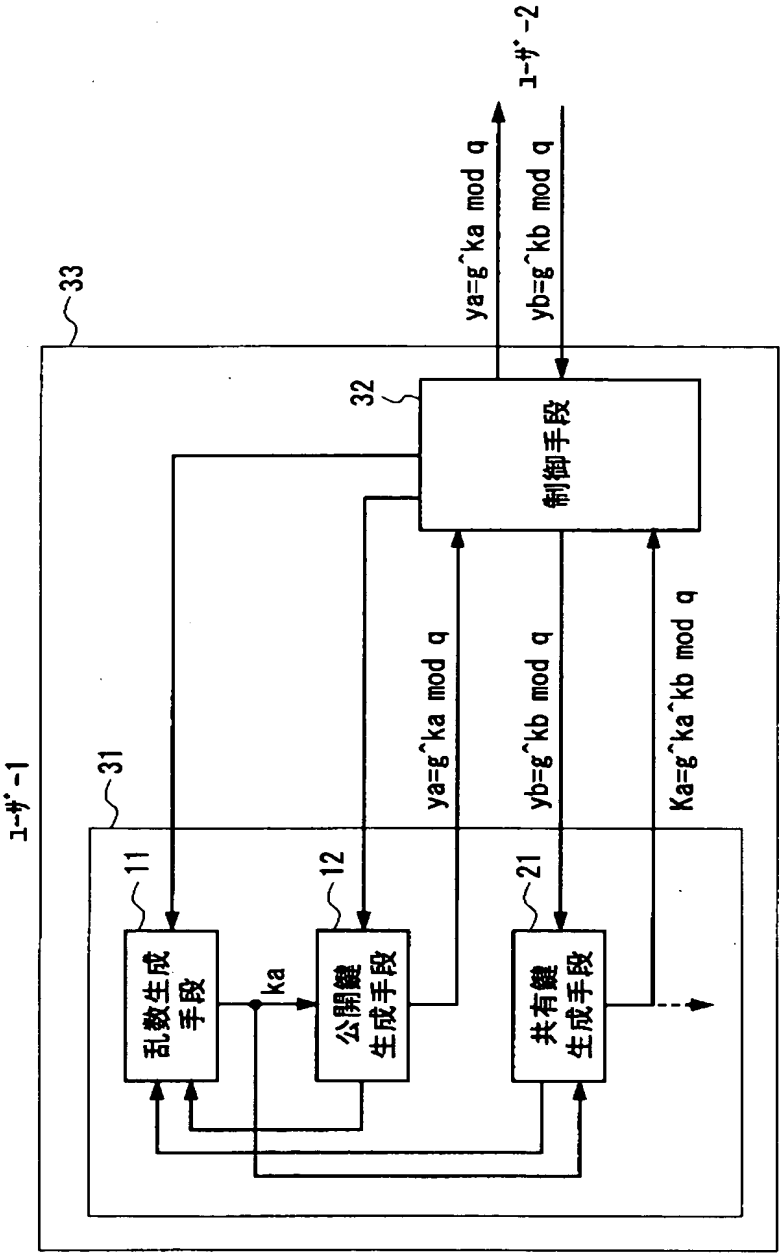
【図１】


ユーザ-1
15
13
11
乱数生成
手段
ka
12
公開鍵
生成手段
14
ya=g^ka mod q
制御手段
ya=g^ka mod q
ユーザ-2

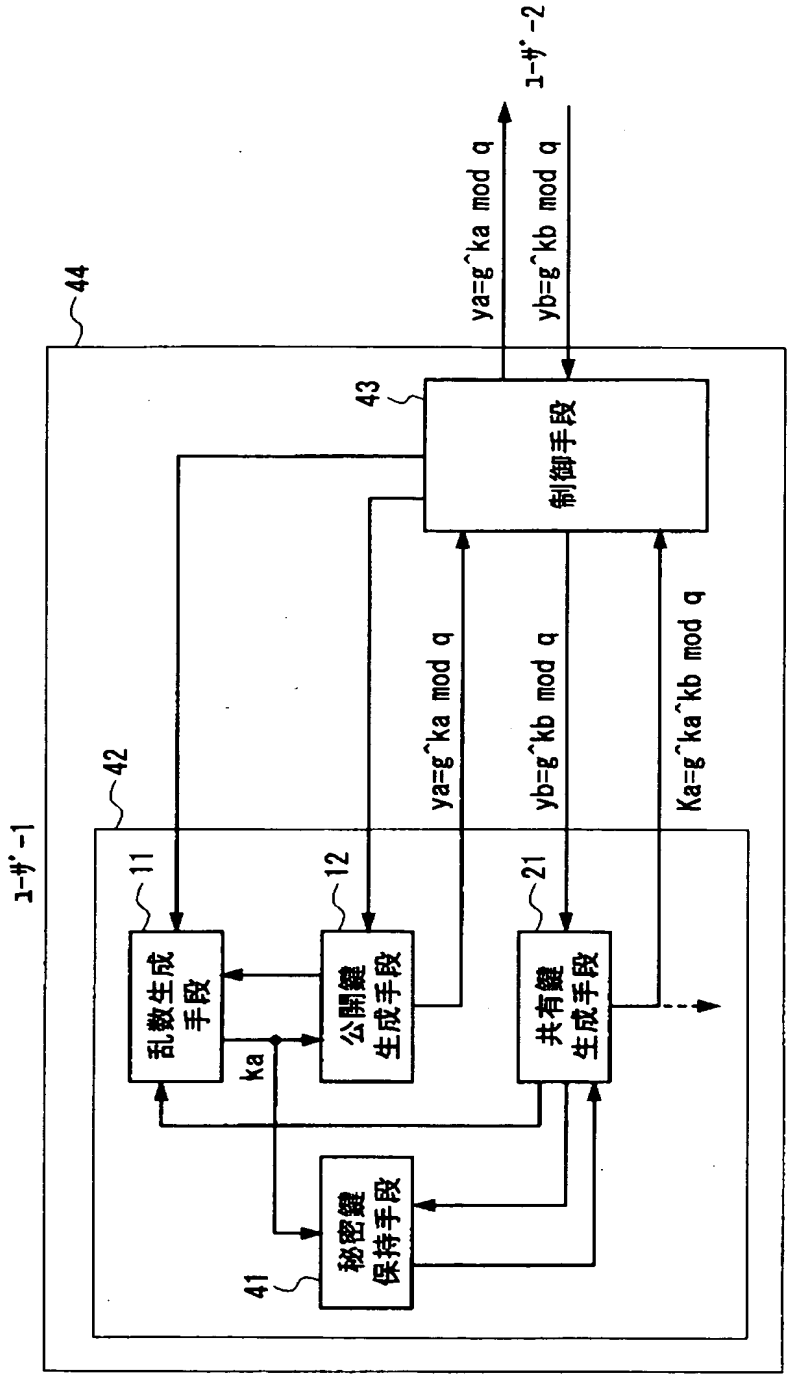
【図２】


ユーザ-2
yb=g^kb mod q
24
23
制御手段
ユーザ-1
22
yb=g^kb mod q
Ka=g^ka^kb mod q
11
21
乱数生成手段
ka
共有鍵生成手段

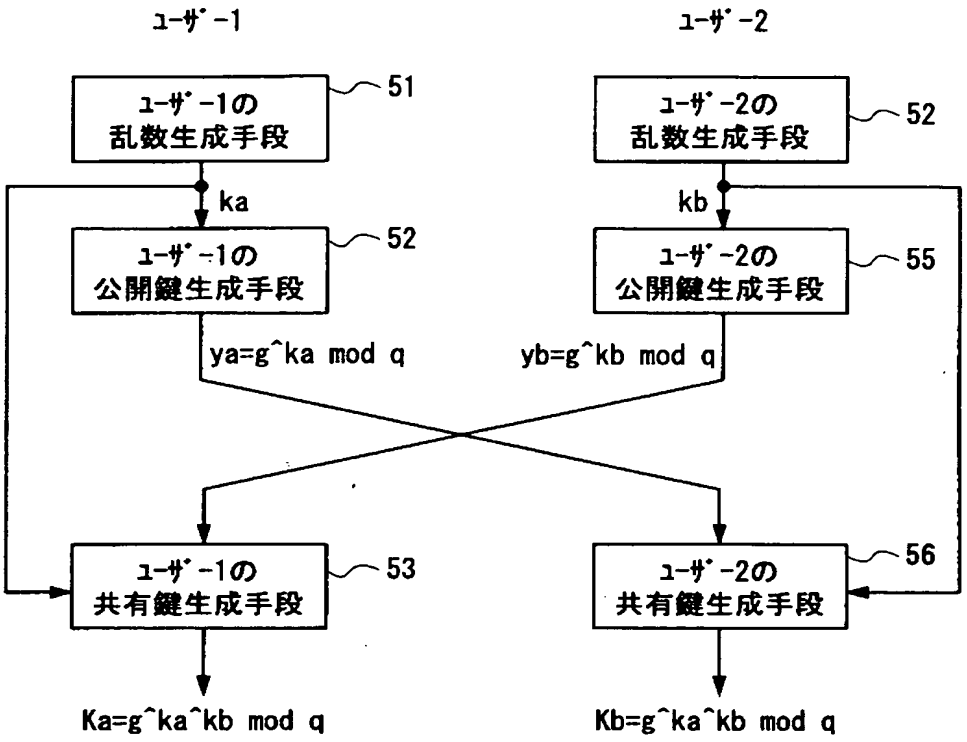
【図３】


ユーザ-2
ユーザ-1
33
32
31
制御手段
乱数生成手段
公開鍵生成手段
共有鍵生成手段
11
12
21
ka
ya=g^ka mod q
yb=g^kb mod q
Ka=g^ka^kb mod q

【図４】


ユーザ-2
ya=g^ka mod q
yb=g^kb mod q
44
43
制御手段
ユーザ-1
42
ya=g^ka mod q
yb=g^kb mod q
Ka=g^ka^kb mod q
11
12
21
乱数生成手段
公開鍵生成手段
共有鍵生成手段
ka
秘密鍵保持手段
41

【図５】


ユーザ-1
ユーザ-2
ユーザ-1の
乱数生成手段
51
ユーザ-2の
乱数生成手段
52
ka
kb
ユーザ-1の
公開鍵生成手段
52
ユーザ-2の
公開鍵生成手段
55
ya=g^ka mod q
yb=g^kb mod q
ユーザ-1の
共有鍵生成手段
53
ユーザ-2の
共有鍵生成手段
56
Ka=g^ka^kb mod q
Kb=g^ka^kb mod q

【書類名】　　要約書

【要約】

【課題】　ＤＨ鍵交換処理時の鍵演算処理を第３者から秘匿し、第３者による装置の流用あるいは改変が極めて困難な公開鍵生成装置，共有鍵生成装置，鍵交換装置及び鍵交換方法を提供すること。

【解決手段】　公開鍵生成装置１５を、乗算が定義された有限群Ｆ上の元をｇ、前記ｇの素数である位数をｑとし０＜ｋａ＜ｑとなる乱数ｋａを生成する乱数生成手段１１、及び前記乱数ｋａと前記元ｇと前記素数ｑより公開鍵ｙａを前記有限群Ｆ上で演算し出力する公開鍵生成手段１２を１つのＬＳＩ１５に集積化し、秘密鍵ｋａがチップ内部で公開鍵ｙａの生成にのみ用いられる構成とし、公開鍵生成装置１５の暗号化演算が外部に漏れないようにする。

【選択図】　　図３

特願２００３－０８８７８８

出　願　人　履　歴　情　報

識別番号　　［０００００５８２１］

１．変更年月日　　１９９０年　８月２８日
［変更理由］　　新規登録
住　所　　大阪府門真市大字門真１００６番地
氏　名　　松下電器産業株式会社